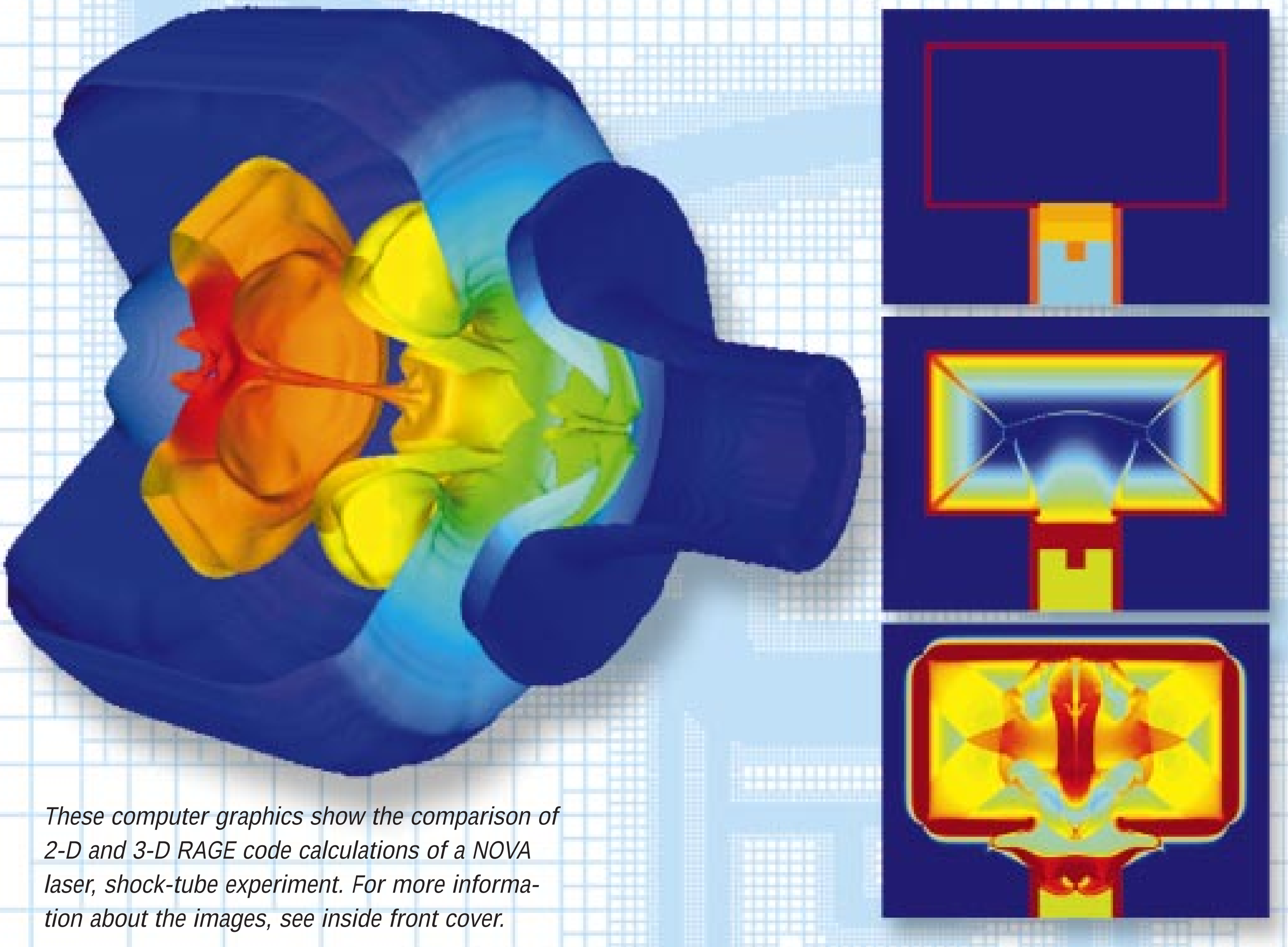
BITS computing&communications news

December 1998

COMPUTING, INFORMATION, AND COMMUNICATIONS (CIC) DIVISION • LOS ALAMOS NATIONAL LABORATORY



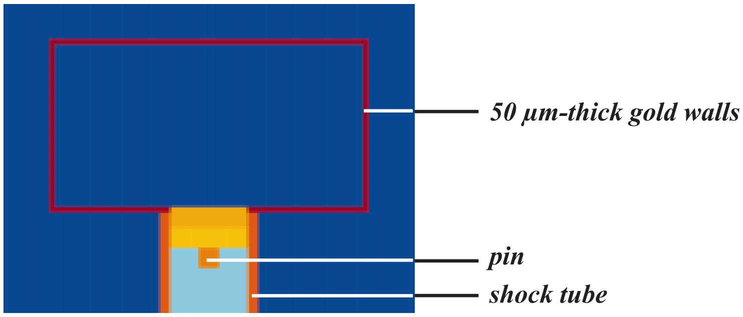
These computer graphics show the comparison of 2-D and 3-D RAGE code calculations of a NOVA laser, shock-tube experiment. For more information about the images, see inside front cover.

Inside this issue

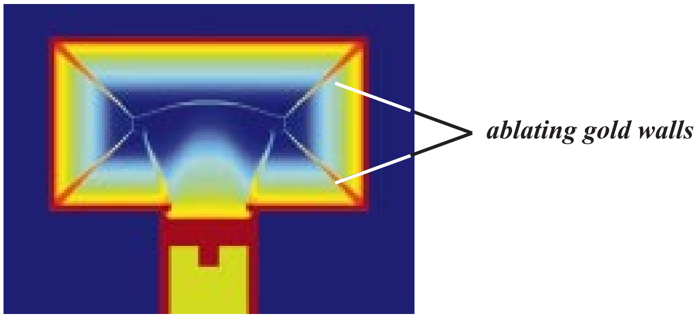
Customer Service Center . . . .(505) 665-4444 or cichelp@lanl.gov

The Customer Service Center page is on the inside back cover of this issue.

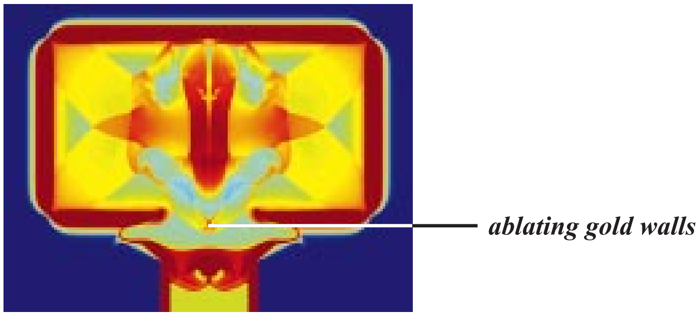
This hohlraum is used to drive a Mach 6 shock into the attached cylindrical shock tube to determine the time evolution of a plastic pin protruding into low-density foam.



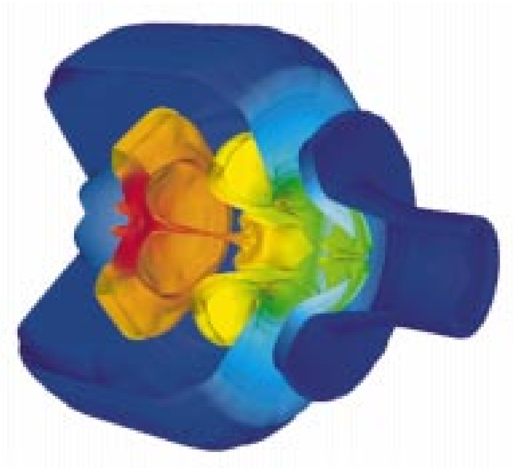
The Eulerian adaptive mesh refinement (AMR) code RAGE is used to simulate these radiation hydrodynamic experiments.



The ablating gold walls interact to form strong jets that send an additional late-time pressure wave into the shock tube.



A relatively coarsely zoned 3-D RAGE calculation of the experiment shows isodensity contours colored by temperature. The code resolves interfaces, shock, radiation fronts, etc. by continuously (cycle-to-cycle) changing the zoning as required. This technique can save as much as a factor of 100 in the number of zones (and therefore computer time) over a non-AMR method. More refined calculations with the actual 3-D geometry will be done on the ASCI Blue Mountain machine.



For more information contact B. Wilde (X-TA), 667-5555 bhw@lanl.gov.

Blue Mountain Is World's Fastest Computer

From a November 10 joint press release

The U.S. Department of Energy (DOE) and Silicon Graphics, Inc. (SGI) today unveiled the world's fastest computer, with the world's most powerful advanced graphics system. The machine, "Blue Mountain," is located at the DOE's Los Alamos National Laboratory (LANL). (Figure 1.) Blue Mountain is the latest advancement in the Energy Department's stockpile stewardship program, which uses science-based methods to assess and certify the safety, security, and reliability of nuclear weapons without underground nuclear testing.

Blue Mountain ran "Linpack," one of the computer industry's standard speed tests for big computers, at a fast, 1.6 trillion floating-point operations per second, giving it a claim to the coveted title, "Fastest Computer in the World."

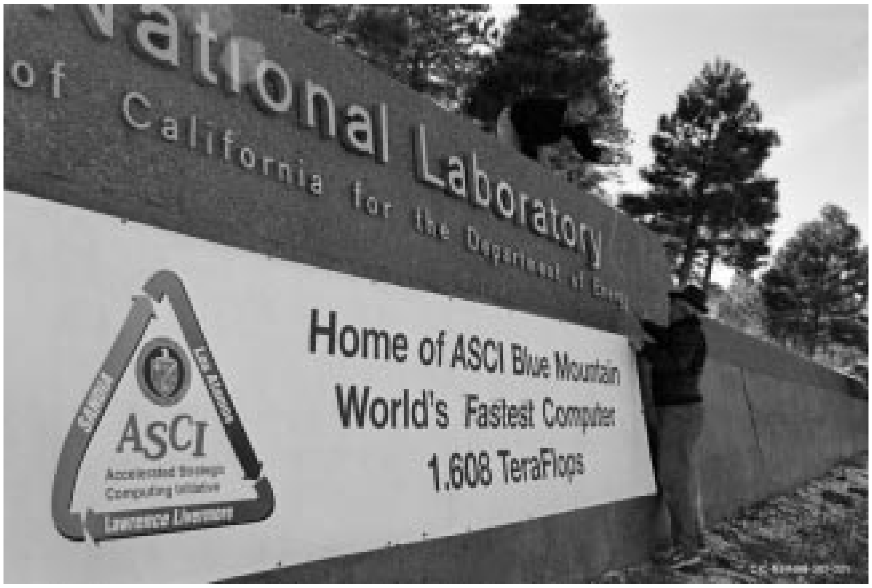
"Blue Mountain and its record-breaking run are great achievements, and I congratulate our Los Alamos and Silicon Graphics team. This is significant progress in our effort to move stewardship of our nation's nuclear weapons from its 50-year foundation in nuclear testing to one based in science and simulation," said Secretary of Energy Bill Richardson. "These high-speed computing tools are necessary to ensure the safety, security, and reliability of the stockpile without underground nuclear testing and help support the U.S. commitment to the Comprehensive Test Ban Treaty. Additionally, high-speed computing and simulation will lead to advances in medicine, manufacturing, automobile safety, and a greater understanding of weather patterns and global climate change."

"We are extremely proud to work with the Department of Energy and Los Alamos to develop the world's fastest supercomputer and advanced visualization system," said Silicon Graphics' Chief Executive Officer Richard Belluzzo. "By working with government on the world's most complex problems, Silicon Graphics is translating that experience into other applications that benefit all of humanity."

"SGI's Blue Mountain is the world's fastest computer and can generate fantastically large amounts of information," said Steve Younger, Associate Lab Director for Nuclear Weapons at LANL. "But once you have trillions of bits of information, you also need the world's most powerful visualization engines to extract knowledge from that data and see it in three dimensions."

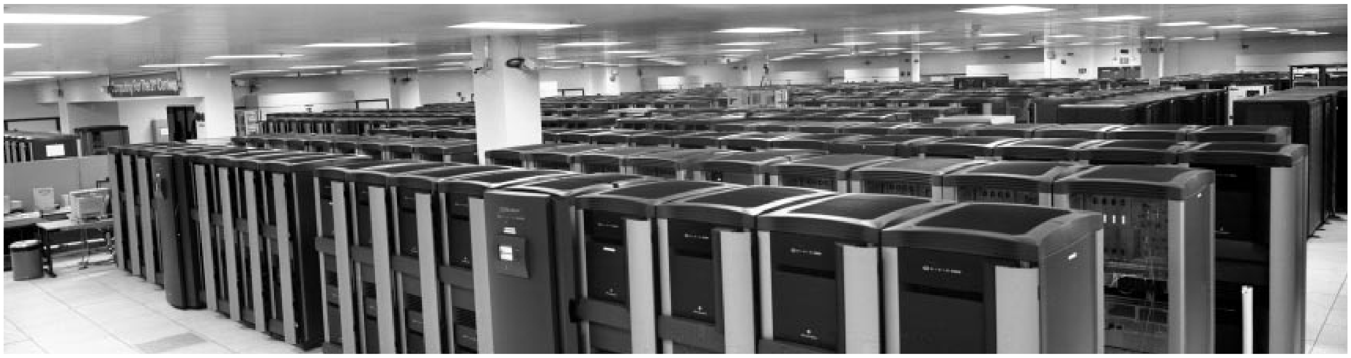
Silicon Graphics has coupled into Blue Mountain the most advanced graphics system in the world, with technology similar to that of the SGI computers used to create the animated scenes in *Antz* and other motion pictures. With this visualization system, answers to complex scientific problems that would have taken weeks or more to display can now be displayed in minutes.

The Blue Mountain computer will give weapons scientists improved scientific tools to analyze the safety and reliability of the nuclear stockpile. During 1999 Blue Mountain is expected to execute 80 million trillion operations over the course of thousands of simulations relating to the nuclear stockpile. This is roughly 10 times more computing than all the calculations executed in support of the U.S. stockpile from the development of the first atomic weapon under the Manhattan Project through 1992, the last year of underground testing. (See Figure 2.)


National Laboratory
of California for the Department of Energy
Home of ASCI Blue Mountain
World's Fastest Computer
1.608 TeraFlops
ASCI
Accelerated Strategic Computing Initiative
Sandia
Los Alamos
Lawrence Livermore

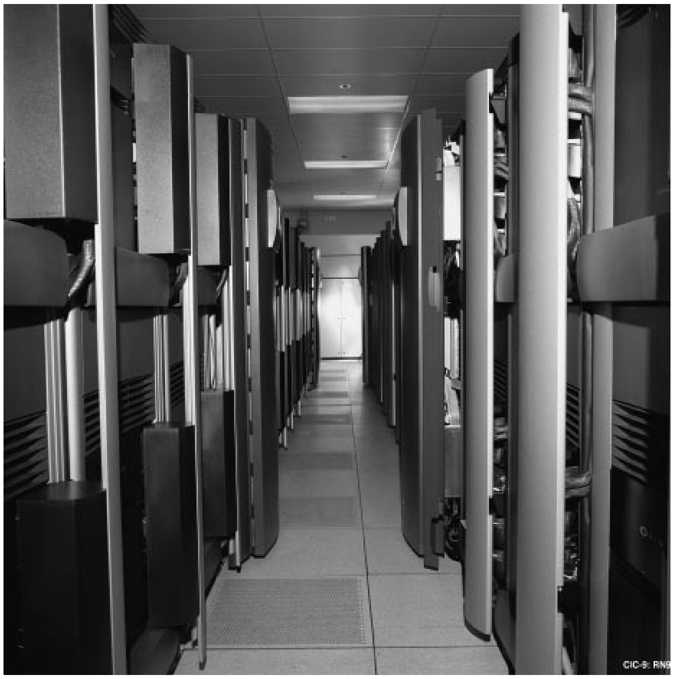
RN#98367021

Figure 1. On Nov. 10 at Los Alamos National Laboratory the U.S. DOE and Silicon Graphics, Inc. announced the world's fastest computer, capable of 1.6 trillion operations per second, and the world's most powerful advanced graphics system. CIC-18's Levi Valencia (on top of the wall) and Kirk Binning hang the banner.



RN#98358019

Figure 2. This room is full of computing machines that comprise "Blue Mountain," presently the world's fastest computer, which is used mainly to characterize the materials and performance of the nation's nuclear weapons without underground nuclear testing.



RN#98357024

Figure 3. The cluster of 48-commercially available Silicon Graphics® Origin2000™ behave as a single computer and communicate with each other at world-record sustained speeds in excess of 650 gigabits per second.

The Department of Energy is developing five generations of high-performance computers as a part of its stockpile stewardship program, with a goal of reaching 100 trillion operations per second by 2004. Blue Mountain is the second of two DOE computers built with a peak speed of at least 3 trillion operations per second. The first, Pacific Blue—developed by IBM and located at DOE's Lawrence Livermore National Laboratory—has not yet been tested on Linpack. The Silicon Graphics Blue Mountain and the IBM-designed Pacific Blue systems use different computer architecture/system designs to reach these high speeds. Both computers were completed ahead of schedule and on budget.

At the heart of Blue Mountain are 48 commercially available Silicon Graphics® Origin2000™ servers containing a total of 6,144 processors. (See Figure 3.) Blue Mountain is organized into 48, 128-processor, shared-memory multiprocessors, or SMPs. The system is designed so the cluster of 48 SMPs—all commercially available servers—behave as a single computer. These 48 SMPs can communicate with each other at world-record sustained speeds in excess of 650 gigabits per second. Blue Mountain's 128-processor, 16-pipe Onyx2™ InfiniteReality® visualization capability is especially valuable because it is an integral part of Blue Mountain, not a separate unit. This visualization capability is twice that of the former record-holding visualization supercomputer, another system developed by Silicon Graphics.

During 1999 Blue Mountain is expected to execute 80 million trillion operations… roughly 10 times more computing than all the calculations executed in support of the U.S. stockpile from…the Manhattan Project through 1992, the last year of underground testing.

Laboratory Unclassified Network Will Implement Changes for Security

Might as well blame it on the Web. “Hacking,” by all rights, should be a proud tradition. Proper hacking involves making computer software work, often by adapting someone else’s program to meet a particular need, and then sharing the results freely with others. It’s a “UNIX-y” way of getting things done, and its examples range from the relatively simple scripts that run the Information Architecture’s discussion archives to the complex but lean Linux operating system.

Unfortunately, the explosive growth of the Web has fostered the growth of a vigorous group of people who claim the name “hacker” but whose goals are fundamentally destructive. Sometimes they want to break into others’ computer systems just to prove that they’re clever enough to do it. Sometimes they’re just pranksters, like the ones who do things like putting up nude images on the CIA’s Web page. Other times they’re more malicious, seeking out trade secrets for competitive advantage or putting up false information that might not be easily recognized as wrong. (Imagine, for example, the type of news release that anti-nuclear activists might like to put on the Laboratory’s home page.)

The Web makes it easier for the whole range of these characters to share the tools they develop for attacking network and machine vulnerabilities. As the attacks become easier, they become more common, which makes them an increasing problem for organizations of all sizes.

As a research institution, our Laboratory has a long history of open collaboration with scientists throughout the world. A side effect of this has been a relatively open unclassified computer network, which evolved to foster these collaborations. The default has been openness, with primary responsibility for security being distributed to the various system administrators. (Note that this applies only to the unclassified network; the secure network has always had very strong protections.)

The growing number of attempted attacks is forcing us to change this model. At the direction of John Browne (see next page), we are now implementing a restrictive network firewall that will shield Laboratory machines from known threats and limit the types of connections that are permitted. By default, Laboratory machines will be behind this firewall. Only a few machines, such as publicly accessible Web servers and/or machines that need to be available to international collaborators, will be outside the firewall.

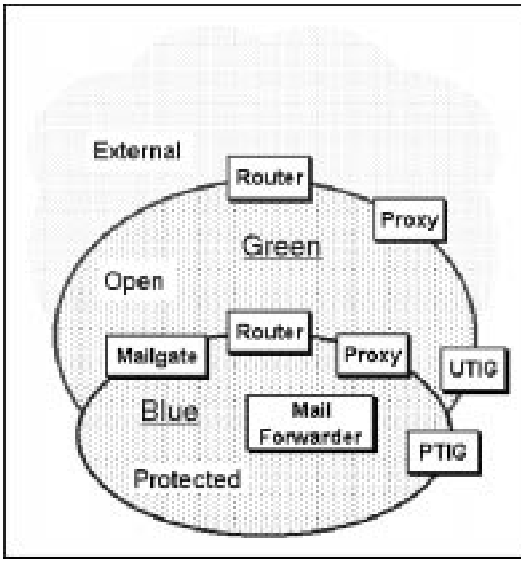
The good news is our computers will be better-protected. The bad news is that some things will inevitably break—certain network connections that are currently simple will become more complex, and some connections might wind up not working at all. Everyone who works at the Laboratory and all of our external collaborators will need to be aware of the changes and make adjustments as needed to operate within the new security model.

This article provides an overview of the new model and the changes it will bring. Additional details are available on the Web, and links are provided in the article.

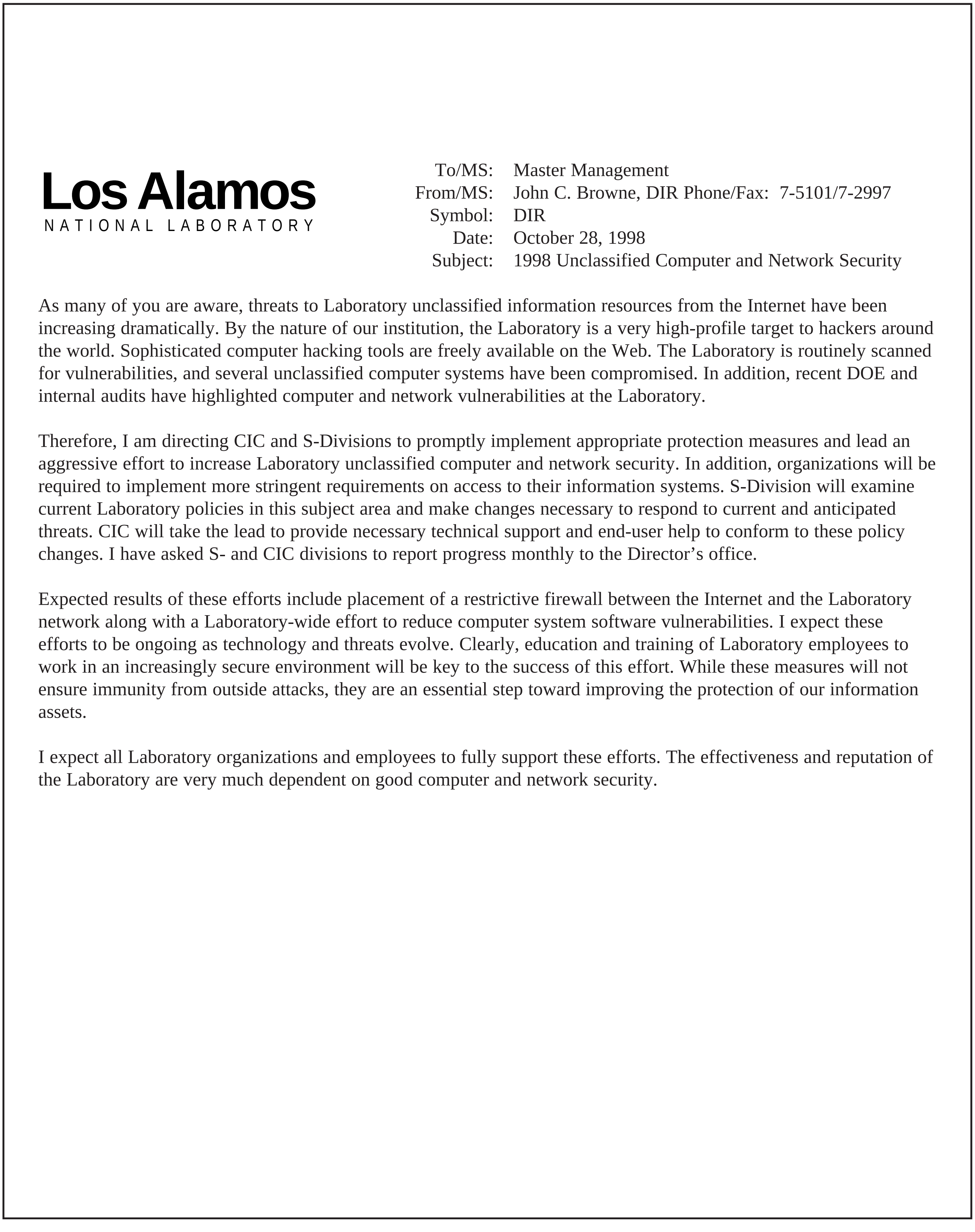
What the New Model Is

The new model is based on the network security model developed by the Information Architecture Project over the past three years. As shown in the illustration below, this model divides the unclassified network into two regions.

- The unclassified open network (or “green” network) is similar to the existing open partition. It has few network-level protections and is intended for machines that need to be easily accessed from external machines (such as publicly accessible Web space).
- The unclassified protected network (or “blue” network) is separated from the external and green networks by a distributed gateway composed of filtering routers, proxies, forwarders, and other mechanisms (see “Tools of the Trade”).



Two regions of the new LANL unclassified network.



Los Alamos
NATIONAL LABORATORY

To/MS:	Master Management
From/MS:	John C. Browne, DIR Phone/Fax: 7-5101/7-2997
Symbol:	DIR
Date:	October 28, 1998
Subject:	1998 Unclassified Computer and Network Security

As many of you are aware, threats to Laboratory unclassified information resources from the Internet have been increasing dramatically. By the nature of our institution, the Laboratory is a very high-profile target to hackers around the world. Sophisticated computer hacking tools are freely available on the Web. The Laboratory is routinely scanned for vulnerabilities, and several unclassified computer systems have been compromised. In addition, recent DOE and internal audits have highlighted computer and network vulnerabilities at the Laboratory.

Therefore, I am directing CIC and S-Divisions to promptly implement appropriate protection measures and lead an aggressive effort to increase Laboratory unclassified computer and network security. In addition, organizations will be required to implement more stringent requirements on access to their information systems. S-Division will examine current Laboratory policies in this subject area and make changes necessary to respond to current and anticipated threats. CIC will take the lead to provide necessary technical support and end-user help to conform to these policy changes. I have asked S- and CIC divisions to report progress monthly to the Director’s office.

Expected results of these efforts include placement of a restrictive firewall between the Internet and the Laboratory network along with a Laboratory-wide effort to reduce computer system software vulnerabilities. I expect these efforts to be ongoing as technology and threats evolve. Clearly, education and training of Laboratory employees to work in an increasingly secure environment will be key to the success of this effort. While these measures will not ensure immunity from outside attacks, they are an essential step toward improving the protection of our information assets.

I expect all Laboratory organizations and employees to fully support these efforts. The effectiveness and reputation of the Laboratory are very much dependent on good computer and network security.

This is the restrictive firewall that the director has called for, and its protections are implemented on a protocol-by-protocol basis. This area is intended for machines that do not need to be freely accessed from external machines (such as most desktop computers), though provisions are made for the machines in the protected network to be able to connect out to external machines.

Throughout this article and other discussions of the security model, “green” is used interchangeably with “unclassified open,” and “blue” with “unclassified protected.”

The original implementation plan was to build the protected network and have organizations voluntarily move into it. By default, machines would be in the green. Decisions would be made at the group-leader level.

The new plan puts machines into the blue by default and requires organizations to petition to move machines into the green. Participation remains voluntary, in that organizations can still move their machines into the green, but decisions are now made at the division director level. The new plan also puts the blue and green onto physically separate network backbones. This makes the wiring somewhat more complicated, in that the two backbones need to be separately wired, but it also makes the network management significantly easier, and it almost certainly makes the new model more reliable.

At the time of this writing, several networks have already been moved into the blue. By the time this article is published, we expect to have two full divisions in the blue. By March 1999, we hope to have the entire Laboratory in the blue (except for those machines that have moved to the green). Hence, anybody who expects to have a need for machines to be in the less restricted green region needs to act quickly.

What the New Model Is Not

- The new model is not directed toward restricting access to information the public is entitled to see nor toward our becoming a more secretive laboratory. Additional protection for sensitive information will be a side effect of the model, but the range of information requiring protection will not expand.
- The new model is not directed toward censorship of employee ideas nor toward restricting employee contacts with international collaborators. Some procedures for electronic communications will become somewhat different, but every effort is being made to enable the Laboratory to continue its business.
- The new model is not by itself adequate for protecting sensitive information. Additional authentication, authorization, and/or encryption is still needed, as appropriate, at the application level.
- The new model is not a guarantee that only authorized people will be on the network. The new model makes it more difficult for unauthorized people to break in, but it does not make it impossible. (For example, an on-site visitor might be “borrowing” an employee’s computer.)
- The new model is not suitable or approved for classified information. The secure network remains physically separate.

Who Will It Affect?

For most Laboratory users, the transition should be nearly transparent. If you currently do your computing from your office machine, connecting to Laboratory machines for most work, using printers on your local network, and connecting to external machines primarily through the Web, then you should hardly notice the change. You will need to set up your Web browser to use the Laboratory proxy (as explained under “How to Cross the Firewall” below), but you’ll still be able to do your work in very nearly the same manner.

Note several caveats, however:

1. Under a separate security initiative, certain Laboratory computing services require single-use passcodes instead of ICN passwords. We currently use secure ID “smartcards” to generate these passcodes. Since that initiative has already been underway for several months, you will have probably already noticed its effects.
2. A few external Web sites might not work correctly if they attempt to use unusual protocols to establish “back door” connections to your machine. These problems will have to be reviewed on a case-by-case basis in order to determine how to address them.
3. It is likely that the POP password you use to check your e-mail will need to be different from the log-in password you use to access the mail server via SSH or telnet. Since POP passwords are easily compromised if unencrypted, we are likely to require that they not be used for anything other than mail.

If you travel and connect back to the Laboratory through the LANL Dial-up Modem Service to check your mail, you should also notice very little change. The dial-in modems will continue to operate as they do today, though a different multiuse password might be required. (We are currently reviewing various options for the modems. They will definitely continue to accept secure ID smartcard passcodes, but the ICN password might be replaced by a separate dial-in password.)

Note: Under a separate initiative, the old “TIG” (terminal internet gateway) is being phased out in favor of the newer 56Kbps US Robotics modems. This affects the phone numbers we dial in to, but not the passcodes/passwords we use. For further details, see the CIC-5 LANL Dial-up Modem Service Web page at <http://www.cic-5.lanl.gov/csc/modems.html>.

If you need to connect to the Laboratory’s protected network from external machines (e.g., DOE or an external Internet service provider) or from a machine in the open region, then you will notice significant changes. You will basically need to provide strong authentication, generally with a secure ID smartcard. In probably the most common scenario, you will first need to log in to a registered machine, from which you can gain access to unregistered machines in the protected region as usual. In addition, several new mechanisms are under development for kerberos, DCE (distributed computing environment), VPN (virtual private network), and other ways of providing authenticated access. Details will be provided as these services become available.

If your machine is in the open region, it will be treated like an external machine if it attempts to access the protected region. You will need to provide authentication as described in the above paragraph. Unlike a user on an external machine, however, you will be able to access many internal-use Web pages directly. Most Information Architecture team areas, for example, will be accessible to both blue and green Laboratory machines.

If you need to use other tools or protocols across the firewall, you are likely to notice changes. As detailed below, many tools need to be somewhat different in their configuration or operation to pass successfully across the firewall.

Tools of the Trade

–“DNS” - A “domain name server,” which translates machine names (e.g., “www.lanl.gov”) into machine-readable IP (Internet protocol) addresses (e.g., “128.165.3.21”). The IP addresses are then used to make the actual connection between machines. By using a different DNS for internal and external traffic, we can obscure internal information from external users.

–“filter” - A mechanism that permits certain network connections while blocking others. Filters are generally routers, though they can also be proxies.

–“firewall” - A combination of filters, proxies, forwarders, and other mechanisms that restrict the flow of network traffic. Acceptable traffic is allowed to pass, while known threats are blocked.

–“forwarder” - A tool, similar to a proxy, that analyzes traffic and changes it if needed before passing it along. For example, a mail forwarder might analyze the sender’s e-mail address and modify it if needed to obscure the internal network structure (“name@abc.lanl.gov” might be changed to “name@lanl.gov”).

–“probe” - A program that tests a network for potential vulnerabilities. Attackers use probes to look for points to attack, while network managers use probes to look for vulnerabilities to correct.

– “proxy” - A tool through which others can establish network connections. For example, with a Web proxy the client sends a request to the proxy, and the proxy forwards the request to the server; the server sends its response to the proxy, and the proxy forwards the response to the client. By standing in the middle of the connection, the proxy is able to provide certain protections to the client. Many proxies operate transparently once the client is correctly configured (e.g., existing bookmarks will continue to work).

–“router” - A tool that “routes” network traffic. When your machine sends a message to another machine, the message is passed through one or more routers that read the address on the message and forward it until it reaches its destination. Many routers are able to filter traffic, permitting certain connections while blocking others.

– “sniffer” - A program that monitors network traffic and captures certain character patterns. Attackers use sniffers to capture name/password combinations, which can then be used for access to other machines, while network managers use sniffers to look for suspicious activity, such as attempted probes.

–“Trojan horse” - A program that, once activated, runs secretly in the background, frequently sniffing network traffic for passwords.

– “users” - The most important part of any security plan. Even the most comprehensive security plan is only as reliable as the users’ behavior.

How to Cross the Firewall

Here is an overview of how to use selected communications protocols across the firewall. Final details are still being worked out for some protocols, and not all protocols are included below, but we hope this overview will serve to provide a taste of how things will operate. Because green and external machines will be treated the same way by the firewall (in almost all cases), the following section will use “internal” to refer to machines behind the firewall (protected network), and “external” to refer to machines outside the firewall (open and external networks).

- Web/HTTP
  - Internal clients can cross the firewall via the Web proxy. (In Netscape Navigator 4.0x, select Edit/Preferences/Advanced/Proxies.
  - Under Manual Proxy Configuration/View, set the proxy to <www-proxy.lanl.gov> and the port to “8002.”)
  - External clients that attempt to access internal servers will be prompted for a user name and secure ID passcode. After a successful log-in, the browser will be permitted through. (A “cookie” is used to maintain state during the session.)
  - Note that a number of pages intended for Laboratory internal use will remain in the open region with only weak protections. These are pages that do not require strong authentication, and they will remain accessible to all Laboratory machines.
- E-mail
  - SMTP will pass freely across the firewall, though transparent filtering and forwarding mechanisms will close common security holes.
  - POP connections from external clients to internal servers will probably need to be made through an SSH tunnel. (See the IA SSH FAQ at <http://www.lanl.gov/projects/ia/stds/lanl/ssh-faq.html>)
  - POP connections from internal clients can cross the firewall freely, though it is important that POP passwords be used only for POP.
- Telnet
  - Telnet from internal clients to external servers is permitted.
  - To telnet from external clients to internal servers, you will need to first log in to a portal with a secure ID passcode. From there you can log in to blue machines.
  - In both of these scenarios, take note that your password can easily be “sniffed” if it is not encrypted (though it would still be difficult for the sniffer to gain the network access needed to log in to an internal machine with a stolen password). Hence, SSH is encouraged for encrypting telnet sessions.
- FTP
  - “Active” mode FTP connections from internal machines are not permitted across the firewall. Instead, use “passive” mode, preferably within SSH forwarding. An outgoing FTP proxy might also be provided.
  - Direct FTP connections from external clients to internal servers are blocked at the firewall. SSH forwarding can be used to establish an encrypted FTP connection into the protected region, and an incoming FTP proxy may be provided.
- NFS
  - NFS is currently under discussion. Most current NFS connections across the firewall will break, which is a good reason to keep people sharing the same file space within the same region. The reason is that most NFS connections use UDP (user datagram protocol), which is inherently vulnerable to attack.
  - Theoretically, NFS read-only mounts from internal servers to external clients should be acceptable, but this may prove impractical to implement without opening an unacceptable hole in the firewall.
  - Theoretically, NFS mounts from external servers to internal clients should be forbidden, but it may prove impractical to attempt to block TCP (transmission control protocol)-based mounts (generally NFS 3). Any user in the protected region who mounts external file space should be very cautious about running any programs in that file space, however, since Trojan horses can easily be planted there.
- Kerberos
  - Kerberos can be passed across the firewall. External users can get their tickets by authenticating with a secure ID passcode.
- Web plug-ins
  - Some Web plug-ins will break when they attempt to communicate across the firewall, generally because they rely on UDP for faster connections. If the plug-in can be configured to use TCP instead (or if it automatically switches to TCP when UDP fails), then it can probably work across the firewall (though there may be other reasons why it is being blocked). We expect some problems here, though we hope to have as many solutions in place as possible before the full implementation is in place.

Again, the above discussion is only an overview. Additional services are under development, and additional protocols are being addressed. For further details and up-to-date news, please visit the Firewall Help page at <http://www.nic.lanl.gov/security/firewall/>.

What Can You Do Today?

Even though the new security model will not be fully implemented until March 1999, there are steps that can be taken today to get ready for the implementation.

- Machines in the Open: Most notably, if you have a machine that you believe needs to be in the open region, contact <firewall-help@lanl.gov> as soon as possible. S-Division has developed a justification form for moving the machine and collecting the required approvals (including your division director's). In addition to the justification and approval, there are technical issues that need to be addressed as soon as possible, including the physical location of the machine and the availability of an open network connection. (Remember, however, that moving a machine into the green will make it more difficult to communicate with machines in the blue.)
- Protected Networks: If you would like to move your network into the protected region before the final implementation (in order to test what will work and what will need to be fixed), also contact <firewall-help@lanl.gov> as soon as possible. As previously noted, certain networks have already been moved, and the experience gained from them will help make the final transition as seamless as possible.
- Web Proxy Now: If you would like to take advantage of the Web proxy before it becomes required, you can go ahead and configure your browser as described under "How to Cross the Firewall." The proxy is already available, and it offers performance benefits such as caching of external pages.

For More Information

The main point of contact for the new network security model is the Firewall Implementors Team, led by CIC-5. The team can be reached via e-mail at <firewall-help@lanl.gov>, and their Web page at <http://www.nic.lanl.gov/security/firewall/> is the best source of detailed, up-to-date information about the new model.

Additional updates and announcements will be posted to the Laboratory home page on a periodic basis, and the Information Architecture Project will be issuing periodic Requests for Help (RFHs) and Requests for Comment (RFCs). (As of this writing, an RFH dealing with dial-in modems is currently under development. By the time this article is published, it may have already been issued. Look to the IA home page at <http://www.lanl.gov/projects/ia/> for details.)

As always, your input is important and valued. The implementation of the new model will mark a significant change in some of the ways that the Laboratory operates. Whether to implement is no longer an open issue, but how to implement and how to do it smoothly are still issues that require open communication among implementors and customers to ensure a successful transition. The transition will happen regardless. If we work together, we can make it work better.

Tad Lane, CIC-1, 505-667-0886,
tad@lanl.govhttp://www.lanl.gov/projects/ia/staff/tad.html
Information Architecture Standards Editor
http://www.lanl.gov/projects/ia/IA
IA Web Team Leader
http://www.lanl.gov/projects/ia-lanl/area/web/

And the Survey Says…

The majority of survey respondents want BITS to do what it has always done and to do it better. They want more of what they are particularly interested in, and they want more convenient access to their items of interest. BITS will continue to be published as hard copy. We will also be changing the Web presentation and instituting an e-mail notification process for those people who would like to connect directly to the on-line BITS. At some point, subscribers will be able to choose the method they prefer for receiving BITS.

Although plans are still evolving and changes take time, you will see a newly designed BITS document, a return to monthly publication, a new editor, and much more content. Each issue will strive for articles and news items concerning supercomputing, infrastructure (Information Architecture, networking, Y2K, etc.), desktop computing issues, and Labwide information systems. BITS will make much more use of the Web so that items of immediate importance can be published. One proposed change that we implemented immediately was the clickable table of contents sent out on e-mail with the announcement of the Oct/Nov issue's URL.

As BITS reaches out to the population it serves (1224 internal subscribers, 460 outside the Lab, 20 in foreign countries, not including all those who access BITS on-line), we will solicit more articles from all users of CIC-Division's services, from the desktop to the ASCI supercomputers. We invite everyone—historians, researchers, enterprise applications users, and others to contribute. If you have an idea that might make an interesting BITS article, please contact Ann Mauzy, 667-5387, mauzy@lanl.gov, or Don Willerton, 5-0424, dxw@lanl.gov.

Some of the CIC-2 people who serve the Laboratory

CIC-2's Future Is in Stewardship, Automation, and “Fun Stuff”

Desktop Group (CIC-2) Group Leader Dale Land predicts that the most important contributions CIC-2 can make to its customers over the next few years involve making desktop computing and the administration of local area networks (LANs) better tools for increased productivity.“We think of the desktop as a window to global information,” Land says. “In this context we will play a leadership role in improving the way users access information. As the integrators of desktop technology, CIC-2 plays a significant role for the Laboratory. This means that point solutions like video conferencing, the Web, and natural-languages interface all roll together into a seamless usable package.”

“One way to improve access to information,” he continues, “is to provide a consistent ‘look and feel’ for information entry points.” He is convinced that the Web browser will be the consistent access point of the future for all kinds of information, whether the user is looking for administrative or scientific data. “Implicit in this,” he continues, “is a security fabric, probably accomplished with some form of “smart-cards,” so systems know who the user is and what information he/she may have access to.” And since we're talking about “blue sky” and the future, Land would like to see a secure system that allows a user to log on once and then have his/her credentials forwarded from session to session.

The next trend for the future is automation, and CIC-2 LAN administrators are already moving in that direction. The object is to be able to put the latest applications, and their patches, on the networked desktops automatically. CIC-2 is working toward ensuring that the desktop environment here at the Laboratory will support this type of automation. Beyond the convenience of keeping a desktop up to date without the owners involvement, automation makes the desktop system much less susceptible to viruses and attacks, and the latest protections can be applied as quickly as they are determined. “We can auto-boost the desktops immune system, if you will,” Land says.

The third trend for the future is to track emerging desktop and networking technology and apply it in such a way that it will increase productivity. “This is the fun part,” Land says. The Web Galaxy project at MIT is investigating the use of voice interface to the Web. No carpal tunnel syndrome from repeated mouse clicks here—just tell your browser what kind of information you seek, and it will form the query and go find it. In another leading-edge effort, Carnegie Mellon University is working on a project to link its students and faculty to the Internet via wireless networking. Picture a student sitting on the lawn outside ivy-covered halls, doing library research right there on her laptop computer. “All this can be done with gigahertz radio technology,” Land explains. “The system uses spread-spectrum, parallel frequencies that make such a conversation difficult to eavesdrop in on.” The security implications, however, would probably preclude using this technology for anything other than the unclassified, open network here at Los Alamos. The technology, at a lower frequency, is being used now for digital cell phones and 900-mHz, spread-spectrum home phones.

“Some of our customers are really pushing us to implement new technology,” says Land. Some customers come back from traveling and tells us about some new technology they have seen and want to know why we don't already have it! Some customers are more comfortable with tried and true technology. We intend to continue to support both,” Land asserts. Our job is to provide cost-effective, highly productive products for the desktop.

It's not easy to keep up with the constant technological change in desktops and networking. The group spends about a half million dollars each year to keep group members trained on new technology. Land foresees a time when group members will be assigned emerging technologies they are interested in, to research and track these technologies and report on them to the group and the Laboratory as a whole.

It's this “whole Laboratory” view that sets CIC-2 group members apart from other network administrators. “We take on a broader, institution-wide perspective in how we offer services, and we tie the services together on a higher level,” says Land. “The group has broad talents, and our customers get the talents and expertise of the whole group (as well as the rest of CIC Division), not just the people on assignment to them.”

“People who work in CIC-2 are attracted to the constant technological change in our business, Land concludes. “These people are very adaptable to change, so I'm confident we will be able to take whatever new technology comes our way in the future and make it work for our customers' increased productivity.”

Land started at the Laboratory as a summer undergraduate student in the former ADP Division. He also worked as a co-op student for IBM General Products Division in Tucson. After earning his BS in Computer Engineering from UNM, he joined ADP full time as a system programmer. He then joined the former C-Division working on a nationwide, secure DOE network. He became one of the founders of the LANL Network Operations Center (NOC) in C-5 (CIC-5). He joined CIC-2 in 1994 as deputy group leader and has recently become the group leader. Dale's hobbies include mountain biking, piano, and acquiring audio/video and other electronic stuff.

Ann Mauzy, mauzy @lanl.gov, (505) 667-5387, Communication Arts and Services (CIC-1).

Some Computing Services Will Be Curtailed during the Holidays

During the Laboratory closure for the Holidays, from 1600, December 24, 1998, through January 3, 1999, some of the computing services normally offered by CIC Division will be unavailable. However, some of these services will be maintained at a minimum operating level. The following sections provide information about specific services.

CM5, SGI/Cray Supercomputers (this includes ASCI), CFS, NFS, and HPSS (Common File System, Network File System, and High Performance Storage System): From 1600, December 24, until 0700, December 26, the CM5, SGI/Cray Supercomputers, CFS, NFS, and HPSS will be unattended. Any problems encountered during this time will not be resolved until after 0700, December 26. From December 26 to January 4, the CM5, SGI/Cray Supercomputers, CFS, NFS, and HPSS will have minimum staffing.

CFS will be unavailable at times, for two-hour periods, from December 26 to January 3, to rebuild the directories.

The open cluster will be left running but will not be supported. This means customers can access and use the cluster, but if they have problems, or if a machine goes down, help will not be available until the Laboratory resumes operations on January 4, 1999.

On December 29 from 0600 to 1800 and on December 30 from 0700 to 1600 some CIC computer services may be unavailable or experience outages. Necessary electrical/mechanical maintenance and upgrades will take place during these time periods. All precautions will be taken to limit the impact on service and to keep the outage as short as possible. Please plan accordingly. For more information call Jim Frybarger at (505) 665-1023 or Rick Rivera at (505) 667-5781.

Up-to-date status will be available by calling (505) 667-2919 or (505) 667-1333.

Research Library Training

The LANL Research Library offers a variety of training opportunities for the Laboratory community. Sessions focus on specialized library databases and other electronic resources. While the sessions listed below will be held at the library, training can be arranged at your site. Contact the Library by phone at 7-4175 or by e-mail to library@lanl.gov, to register for a session or to arrange a special session/training at your site.

Date	Time	Subject Matter
1/6/99	1:00-1:30	Introduction to Electronic Library Resources
1/6/99	1:00-1:30	Research Library Tour
1/11/99	1:00-1:30	SciSearch® Alerting Service
1/13/99	1:30-2:00	Finding Addresses and Phone Numbers on the WWW
1/20/99	1:00-1:30	Research Library Tour
1/20/99	1:30-2:00	Introduction to Electronic Library Resources
1/21/99	2:00-4:00	InfoSurfing: Basic Web Searching Strategies
1/28/99	1:00-1:30	Grants & Funding on the WWW

Engineering Index Is Now Available from the Research Library

Engineering Index® at LANL, the world’s most comprehensive interdisciplinary engineering database, is now available from the Research Library. Engineering Index has more than four million records, covering 1969 to the present and is updated weekly. Each year, more than 220,000 new records with abstracts are added from more than 2,600 international journals, numerous conference proceedings, technical reports, and dissertations. Subject coverage spans more than 175 disciplines and major specialties within engineering. Hyperlinks are provided when the material is available in full-text on the World Wide Web; if the Library has the material in print form, that is indicated also.

Engineering Index at LANL is accessible in Web and telnet versions, and is included in the “top databases” box on the Electronic Databases page.

Computer Training

The Customer Service Group (CIC-6) offers technical computer training (enterprise information applications, communications, office administration, and Web authoring) and advanced technical computer training (programming languages, system administration, and advanced applications). To register for a course access our Web page at
http://www.lanl.gov/cic/cic6/training.html

Or from the LANL home page select the links: Training, Computer. For further information about technical computer training call (505) 667-9559, and for advanced technical computer training call (505) 667-9399.

Communications

- Eudora 4.02
- Lotus Notes 4.5x
- Meeting Maker 5.0.3

Office Skills 2000

- Office Skills 2000 LANL Computing
- Office Skills 2000 Professional Development

Web Authoring and Browsing

- FrontPage 98
- HTML Basics
- HTML Intermediate
- Netscape 4.0

Coming Soon

- Directory Information System (DIS) Web
- Procurement Desktop
- Recharge

Enterprise Information Applications (EIA)

- Data Warehouse - Basics
- Data Warehouse EDS Reports
- EDS Basics
- EDS Training Plans
- Foreign Travel GUI
- Infomaker
- Invoice Approval System
- Purchase Card System
- Time & Effort GUI
- Travel GUI
- Web JIT

Other EIA Courses

- Financial Management Information System (FMIS)
- Property Accounting, Inventory and Reporting System (PAIRS)
- Signature Authority System (SAS)
- Secretarial/Contract Services (SE)
- Salary Review System (SRS)
- Directory Information System (DIS)
- Automated Chemical Information System (ACIS)

Application Training

- Advanced WWW Development
- FrameMaker Basic & Advanced
- Foundations of IDL Programming
- IDL 5.0 Graphic Object Workshop
- Netscape Servers for Intranet Development
- Origin2000 Applications Programming and Optimization
- Sendmail/Managing Internet Mail
- C++ and the Unified Modeling Language
- Sybase Performance and Tuning for System 11
- Sybase SQL Server Administration
- Unix (Beginning)
- Unix (Advanced)
- Visual Basic 5.0 Fundamentals
- Visual C++ Windows Programming

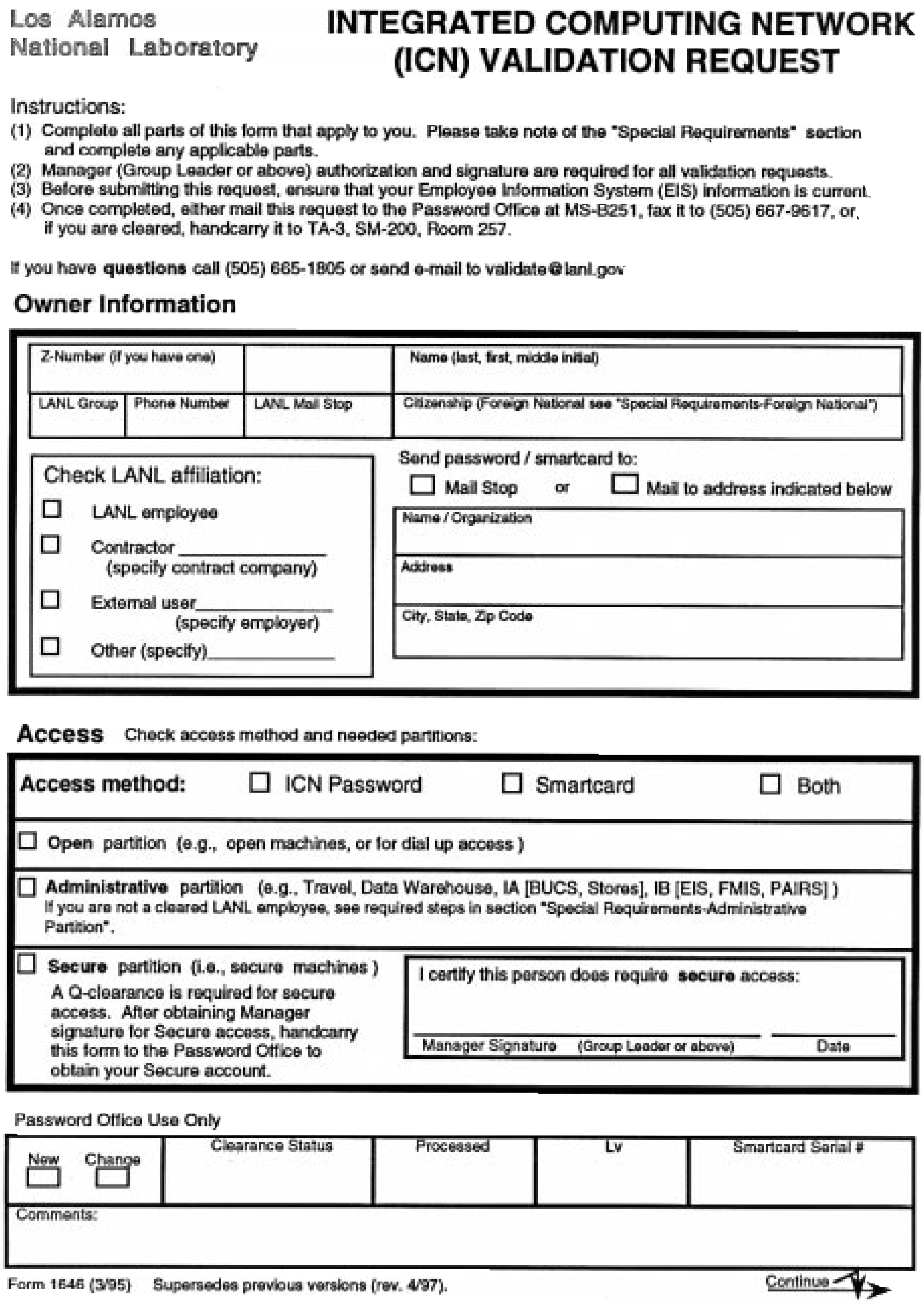
Programming Training

- C Programming (Beginning)
- C Programming (Advanced)
- C++ for Experienced C Programmers
- ANSI/ISO C++ Programming Clinic (Advanced C++)
- Java Programming
- Java Programming Workshop
- Distributed Programming With Java
- Object Technology: A Management Overview
- Object-Oriented Analysis and Design
- Perl Programming
- C-Shell Programming
- Programming or Beginners Using Java

System Administration Training

- SGI System Administration (Beginning)
- SGI System Administration (Advanced)
- SGI Network Administration
- SGI Performance Evaluation and System Tuning
- Solaris 2.X System Administration
- Solaris 2.X Network Administration
- Solaris 2.X Server Administration
- Unix and Windows NT Integration
- Windows NT Workstation and Server
- Windows NT Optimization and Troubleshooting
- Windows NT Security

cut along dashed line



Los Alamos
National Laboratory

INTEGRATED COMPUTING NETWORK (ICN) VALIDATION REQUEST

Instructions:

(1) Complete all parts of this form that apply to you. Please take note of the "Special Requirements" section and complete any applicable parts.
(2) Manager (Group Leader or above) authorization and signature are required for all validation requests.
(3) Before submitting this request, ensure that your Employee Information System (EIS) information is current.
(4) Once completed, either mail this request to the Password Office at MS-B251, fax it to (505) 667-9617, or, if you are cleared, handcarry it to TA-3, SM-200, Room 257.

If you have **questions** call (505) 665-1805 or send e-mail to validate@lanl.gov

Owner Information

Z-Number (if you have one)			Name (last, first, middle initial)
LANL Group	Phone Number	LANL Mail Stop	Citizenship (Foreign National see "Special Requirements-Foreign National")

Check LANL affiliation:

□ LANL employee

□ Contractor ______________
(specify contract company)

□ External user______________
(specify employer)

□ Other (specify)______________

Send password / smartcard to:

□ Mail Stop or □ Mail to address indicated below

Name / Organization

Address

City, State, Zip Code

Access Check access method and needed partitions:

Access method: □ ICN Password □ Smartcard □ Both

□ **Open** partition (e.g., open machines, or for dial up access)

□ **Administrative** partition (e.g., Travel, Data Warehouse, IA [BUCS, Stores], IB [EIS, FMIS, PAIRS])
If you are not a cleared LANL employee, see required steps in section "Special Requirements-Administrative Partition".

□ **Secure** partition (i.e., secure machines)
A Q-clearance is required for secure access. After obtaining Manager signature for Secure access, handcarry this form to the Password Office to obtain your Secure account.

I certify this person does require **secure** access:

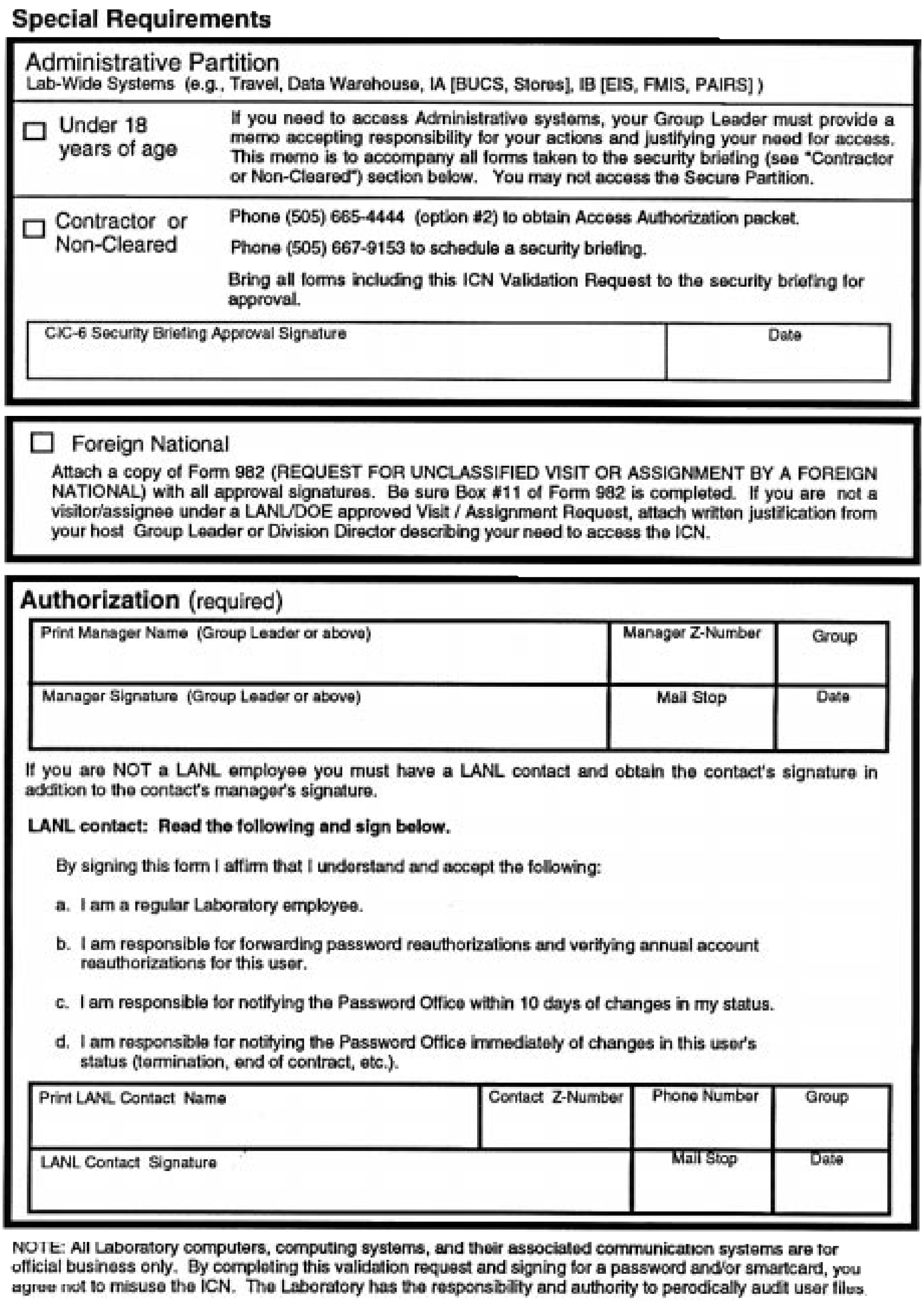
______________________________ ______________
Manager Signature (Group Leader or above) Date

Password Office Use Only

New □ Change □	Clearance Status	Processed	Lv	Smartcard Serial #
Comments:				

Form 1646 (3/95) Supersedes previous versions (rev. 4/97).

Continue



Special Requirements

Administrative Partition

Lab-Wide Systems (e.g., Travel, Data Warehouse, IA [BUCS, Stores], IB [EIS, FMIS, PAIRS])

□ Under 18 years of age

If you need to access Administrative systems, your Group Leader must provide a memo accepting responsibility for your actions and justifying your need for access. This memo is to accompany all forms taken to the security briefing (see "Contractor or Non-Cleared") section below. You may not access the Secure Partition.

□ Contractor or Non-Cleared

Phone (505) 665-4444 (option #2) to obtain Access Authorization packet.

Phone (505) 667-9153 to schedule a security briefing.

Bring all forms including this ICN Validation Request to the security briefing for approval.

CIC-6 Security Briefing Approval Signature	Date

□ Foreign National

Attach a copy of Form 982 (REQUEST FOR UNCLASSIFIED VISIT OR ASSIGNMENT BY A FOREIGN NATIONAL) with all approval signatures. Be sure Box #11 of Form 982 is completed. If you are not a visitor/assignee under a LANL/DOE approved Visit / Assignment Request, attach written justification from your host Group Leader or Division Director describing your need to access the ICN.

Authorization (required)

Print Manager Name (Group Leader or above)	Manager Z-Number	Group
Manager Signature (Group Leader or above)	Mail Stop	Date

If you are NOT a LANL employee you must have a LANL contact and obtain the contact's signature in addition to the contact's manager's signature.

LANL contact: Read the following and sign below.

By signing this form I affirm that I understand and accept the following:

a. I am a regular Laboratory employee.

b. I am responsible for forwarding password reauthorizations and verifying annual account reauthorizations for this user.

c. I am responsible for notifying the Password Office within 10 days of changes in my status.

d. I am responsible for notifying the Password Office immediately of changes in this user's status (termination, end of contract, etc.).

Print LANL Contact Name	Contact Z-Number	Phone Number	Group
LANL Contact Signature		Mail Stop	Date

NOTE: All Laboratory computers, computing systems, and their associated communication systems are for official business only. By completing this validation request and signing for a password and/or smartcard, you agree not to misuse the ICN. The Laboratory has the responsibility and authority to perodically audit user files.

cut along dashed line

Reader Feedback

Feedback helps us to provide a document that responds to the changing needs of its readership. If you have comments or questions about this publication, please let us hear from you. We have reserved the back of this form for that purpose. We also accept articles for publication that are of interest to our readers. Contact the managing editor for more information. This form is also used for new subscriptions, deletions, or changes. Instructions are on the back. If you prefer to contact us by e-mail, send your comments and/or subscription request to mauzy@lanl.gov.

Do Not Staple
Fold on This Line First

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL
FIRST-CLASS MAIL PERMIT NO. 88 LOS ALAMOS NM

POSTAGE WILL BE PAID BY THE ADDRESSEE

MAIL STOP D416
ATTN: ANN MAUZY, INTERIM EDITOR
CUSTOMER SERVICE GROUP (CIC-6)
LOS ALAMOS NATIONAL LABORATORY
PO BOX 1663
LOS ALAMOS NM 87544-9916

Do Not Staple, Seal with Tape
Fold Here

Feedback

New Subscriptions, Deletions, and Changes

BITS is published by Los Alamos National Laboratory. If you would like to be added to or deleted from our mailing list, please check the appropriate line, complete the form below, and mail us the form.

_______ Add my name to the **BITS** mailing list.

_______ Delete my name from the **BITS** mailing list.

_______ Change my name/address as indicated below.

Name		Date
Address		Mail Stop
Group	Organization	
City	State	Zip
Phone	Number of copies	Employee Z#

1998 12-MONTH INDEX

For a more complete index, see <http://www.lanl.gov/Internal/divisions/cic/publications.html>

Keywords	Title of BITS Article	Date	Page
ASCI	*Blue Mountain Is World’s Fastest Computer*	*Dec. ’98*	*1*
BITS Interviews	*Charlie Slocomb*	*Feb. ’98*	*1*
	Mary Moore	*Mar. ’98*	*1*
	Rick Luce	*Apr. ’98*	*1*
		J/J. ’98	*5*
	Gary Clark	*J/J ’98*	*2*
	John Blaylock	*A/S ’98*	*2*
	Chris Kemper	*A/S ’98*	*8*
	Bob Newell	*O/N ’98*	*1*
	Earleen Eden	*O/N ’98*	*3*
	Dale Land	*Dec. ’98*	*11*
BIOSIS at LANL	*BIOSIS at LANL Database Available from the Research Library*	*Feb. ’98*	*13*
Business Systems	*The Next Step for LANL Business Systems*	*Feb. ’98*	*6*
CIC (Computing, Information, & Communications)	*[CIC] Division Leader Gives “30,000-Foot View” for the Next Five Years*	*Feb. ’98*	*1*
CIC-1	*CIC-1 Communicates in Words, Pictures, and Pixels*	*Mar. ’98*	*1*
CIC-2	*CIC-2’s Future Is in Stewardship, Automation, and “Fun Stuff”*	*Dec. ’98*	*11*
CIC-10	*CIC-10: “Knowledge Is Our Most Important Product”*	*O/N ’98*	*3*
CIC-12	*CIC-12 Moves Into Software Quality Assurance, Needs Scientific Programmers*	*J/J ’98*	*2*
CIC-14	*CIC-14 Becomes a Bridge to Human Knowledge*	*Apr. ’98*	*1*
	Library Without Walls Anticipates Its Next Generations	*J/J ’98*	*15*
Deskstop Computing	*CIC-2’s Future Is in Stewardship, Automation , and “Fun Stuff”*	*Dec. ’98*	*11*
Desktop-Computing Costs	*Eye-Opening Reports About Desktop Computing Costs*	*J/J. ’98*	*10*
Electronic Journals	*Accessing Electronic Journals for Research in Computer Science*	*Feb. ’98*	*12*
E-mail	*MacTips: Dealing with [E-mail] Attachments in Eudora Pro*	*Aug. ’97*	*16*
	E-Mail Server Now Available in the Secure Network	*Feb. ’98*	*8*
ESD	*ESD Provides Unexpected Software Savings*	*Feb. ’98*	*8*
Filters	*Content Labeling and Signing: Getting Ready for Filters*	*Apr. ’98*	*10*
Fraud Detection	*Detecting Tax and Medicare Fraud*	*J/J ’98*	*4*
GeoRef	*GeoRef Now Available at Your Desktop*	*Feb. ’98*	*13*
HPCwire	*Lab Considers Group Subscription for HPCwire*	*Apr. ’98*	*4*
Image Compression Standard	*The Image Compression Standard for Fingerprints*	*Mar. ’98*	*6*
Information Systems	*Engineering Index Is Now Available from the Research Library*	*Dec. ’98*	*13*
JavaScript	*JavaScript Observations and Tips: Part II*	*May ’97*	*11*
	Enabling Cookies and JavaScript on Netscape	*Mar. ’98*	*5*
Labwide Systems	*Customer Feedback Guides Improvements to Labwide Systems*	*Aug. ’97*	*4*
	Avoiding Print Problems on Labwide Systems	*Feb. ’98*	*10*
Newell, Bob	*24 Years Later, Bob Newell Joins the Lab as Deputy CIC Division Director*	*O/N ‘98*	*1*
Networks	*Laboratory Unclassified Network Will Implement Changes for Security*	*Dec. ’98*	*3*
PNG	*It's Time for PNG: A Graphics Format You Can Pronounce*	*O/N’98*	*7*
Popular Science Award	*PS Awards LANL Web*	*O/N ‘98*	*12*
Radiation Transport	*Unstructured-Mesh Radiation Transport*	*J/J ’98*	*1*
RAGE	*The Los Alamos RAGE Code: Scalable, Parallel Performance*	*Apr. ’98*	*5*
Records Management	*CIC-10: “Knowledge Is Our Most Important Product”*	*O/N ‘98*	*3*
Supercomputing	*Blue Mountain Is World’s Fastest Computer*	*Dec. ’98*	*1*
TeleFlex and GWIS	*TeleFlex and GWIS*	*Feb. ’98*	*4*

Keywords	Title of BITS Article	Date	Page
UNICOS	*Transition of Machine Gamma to UNICOS 9.0.2.6*	*Mar. ’98*	*5*
Wildfires	*Forecasting Wildfires and Other Crises*	*Apr. ’98*	*3*
World Wide Web (WWW or Web)	*Research Library’s WWW Online Catalog Improved*	*Nov. ’97*	*10*
	Extending Web Documents: Getting Ready for XML	*Mar. ’98*	*8*
	Tips for Desktop Users Available on the Web	*Apr. ’98*	*8*
	Enterprise Information Applications Available on the Web	*J/J ’98*	*8*
	Research Library Now Offering INSPEC Database	*J/J ’98*	*9*
	It’s Time for PNG: A Graphics Format You Can Pronounce	*O/N ‘98*	*7*
Year 2000 (Y2K)	*System Layers and the Year 2000*	*Mar. ’98*	*3*

Customer Service Center . . . . . .(505) 665-4444 or cichelp@lanl.gov

Because of the wide variety of CIC computing services, numerous facilities are available to address your questions. If you are uncertain whom to call, you can always call the Customer Service Center (CSC). CSC consultants are trained to either answer your question or locate someone who can. To reach the appropriate consultant, dial 665-4444 and make your selection from the following choices:

Option 1: New user topics including e-mail, passwords, registration, and World Wide Web.

Option 2: Labwide Systems such as Travel, Time and Effort, and Purchase Cards.

Option 3: Scientific computing, storage systems, and networking.

Option 4: Classroom instruction and training.

Option 5: Desktop Consulting for PC and Macintosh software and network configurations.

Consulting Via E-Mail

Customer Service Center	cichelp@lanl.gov
Scientific and engineering computing	consult@lanl.gov
Administrative and business computing	labwide@lanl.gov
Passwords and registration	validate@lanl.gov
Macintosh computing	Mac-help@lanl.gov
PC computing	PC-help@lanl.gov
UNIX computing	UNIX-help@lanl.gov

Other Useful Numbers

Advanced Computing Laboratory	665-4530
Central Computing Facility	667-4584
Network Operations Center	noc@lanl.gov or 667-7423
Telephone Services Center	667-3400

Produced by the Computing, Information, and Communications (CIC) Division

Interim Editor: Ann Mauzy 667-5387, mauzy@lanl.gov (CIC-1)

Design: Chris J. Lindberg and Wendy Burditt (CIC-1)

Illustration: Dave Delano

Printing: Imaging Services Group (CIC-9)

Los Alamos National Laboratory, an affirmative action/equal opportunity employer, is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36.

All company names, logos, and products mentioned herein are trademarks of their respective companies. Reference to any specific company or product is not to be construed as an endorsement of said company or product by The Regents of the University of California, the United States Government, the U.S. Department of Energy, nor any of their employees. The Los Alamos National Laboratory strongly supports academic freedom and a researcher's right to publish; therefore, the Laboratory as an institution does not endorse the viewpoint of a publication or guarantee its technical correctness.

Los Alamos
NATIONAL LABORATORY

Los Alamos
NATIONAL LABORATORY

Los Alamos, New Mexico 87545

BITS is published bimonthly to highlight recent computing and communications activities within the Laboratory.
We welcome your suggestions and contributions.

BITS can be accessed electronically via the following URL:

http://www.lanl.gov/cic/publications.html

LALP-98-28 (12-98)